Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Questfire Energy Corp. (Organization)
Decision number (file number)	P2016-ND-44 (File #002092)
Date notice received by OIPC	January 5, 2016
Date Organization last provided information	April 5, 2016
Date of decision	August 17, 2016
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • earnings figures, • bank account number, • Social Insurance Number, and • date of hire. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	

Description of incident	• The Organization uses a third party payroll service provider. • On December 24, 2015, the service provider sent a package of summary reports and employee pay stubs to the Organization by courier. However, the package was stolen from the courier truck as it was making deliveries. • The service provider notified the Organization about the incident on December 29, 2015. • On or around April 2015, the service provider recovered a portion of the stolen information that had been discarded in a downtown parking lot. • The Organization confirmed that bank account numbers, social insurance numbers and hire dates for all employees were recovered. Employee pay stubs (including names, addresses and earnings figures) were not recovered.
Affected individuals	There are 28 affected individuals.
Steps taken to reduce risk of harm to individuals	• Notified police services. • Advised employees to contact their banks about the incident, and to monitor transactions. • Advised employees to contact credit reporting agencies.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 30, 2015 and through a "Staff Meeting" on January 4, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported that the information at issue could possibly be used for identity theft and access to an employee's personal bank account. I agree with the Organization. The personal information at issue includes sensitive identity and financial information that could be used to cause the harms of identity theft and fraud or financial loss. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that it was likely the incident was a random act and not a targeted attempt to steal payroll information. The Organization advised employees to contact the credit reporting agencies, and also reported that most of its employees were advised by their banks that it was not necessary to change their banking information. After a portion of the information was recovered (including the most sensitive identity information and financial information for all affected employees), the Organization reported increased

	confidence that sensitive information was no longer in the public domain. However, the Organization could not be completely sure this was the case, as, although unlikely, the information might have been copied. In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft), indicating malicious intent. Although I agree with the Organization that the recovery of a portion of the information mitigates the risk of harm somewhat, I am concerned that the information was exposed for approximately three months.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The personal information at issue includes sensitive identity and financial information that could be used to cause the significant harms of identity theft and fraud or financial loss. The likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft), indicating malicious intent. Although I agree with the Organization that the recovery of a portion of the information mitigates the risk of harm somewhat, I am concerned that the information was exposed for approximately three months.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email on December 30, 2015 and through a "Staff Meeting" on January 4, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner